IN THE SPECIFICATION:

On page 3, line 31, to page 4, line 8, amend the paragraph to read as follows:

The present invention therefore addresses instances where the issue is not merely whether the information is authentic, but rather whether the information is authentic (and unaltered), and the copy itself an original. Obviously, known techniques may be used to authenticate the content of a document, for example, by providing self-authenticating digital signatures, remote database authentication, trusted intermediary techniques, and the like. Likewise, numerous techniques are available for providing self-authenticating features for the physical medium, for example, security threads, inks, papers and watermarks, printing techniques (e.g., intaglio printing, microlithography), fluorescent inks and/or fibers, ~~stenangiographic~~ steganographic patterns, magnetic and/or electrical/electronic patterns, and the like.

B1

On page 48, amend lines 1-22 to read as follows:

According to another embodiment of the invention, a document stock is provided with a substantially irregular

B2

color pattern on a microscopic scale, but having a uniform average background reflection. Therefore, attempts to copy the document will require that the background be subtracted, and the forgery placed on a clean piece of similar stock. This provides the opportunity to ~~stenangiographically~~ steganographically hide pseudorandom image information in the image microstructure of the document, using techniques which are essentially invisible. For example, if the stock includes a relatively high density of light colored cellulose fibers, a sparse pattern of dots could be printed on the stock using the same dye. Therefore, it would be difficult or impossible to analyze every color portion of the document to distinguish fibers from printed dots; however, the document could be authenticated by knowing the imposed locations of the dots. Simple photocopying of the document with the fiber and dot pattern would be ineffective since visually, the gross appearance would be different from an authentic document. This has the advantages that the stock need not be scanned during manufacture to determine the pattern, that a simple mask or set of masks (e.g., dots and voids) could be used for authentication, and that the stock precustomization may be distributed and decentralized.

cont BV

Advantageously, an optical mask is formed using a transmissive liquid crystal light shutter overlayed on the document. In this manner, a first mask defines dot locations, a second mask defines locations which should have no dots (but may have fibers), a third mask defines a printed document content, and a fourth mask defines locations which should have no content, all of which may be visually confirmed. Thus, for authentication, the document code is used to call up an associated database record, or the self-authentication codes read. This defines the four masks, which are applied sequentially to the light shutter.

On page 54, line 26, to page 55, line 15, amend the paragraph to read as follows:

The apparently non-deterministic characteristic may, for example, also comprise a deterministic characteristic which is hidden, i.e., a ~~stenangiographic~~ steganographic code. In this case, a sparse pattern generated by a pseudorandom code may be provided. This code may be imprinted separately from or together with the document content. In order to make the ~~stenangiographic~~ steganographic characteristic counterfeit resistant, it is

preferably hidden in a feature of the medium. Thus, if a counterfeiter seeks to copy the counterfeit resistant document in sufficient detail to include the ~~stenangiographic~~ steganographic code, the copy will also include features intrinsic to the medium, resulting in a requirement for use of a corresponding medium which is, itself, absent any conflicting features, a requirement which may be made very difficult by selection of the stock. If the counterfeiter seeks to copy only the apparent document features, the ~~stenangiographic~~ steganographic code will be filtered, and thus absent from the copy. Thus, the apparently non-deterministic characteristic may be imprinted on the document in deterministic fashion. Alternately, the apparently non-deterministic characteristic may be truly non-deterministic, i.e., the result of random and irreproducible processes and effects, and for example, may be intrinsic to the medium substrate. Accordingly, a unique identifier of the document may comprise a serial number, and the apparently non-deterministic characteristic comprises a pseudorandom copy-resistant printed marking, wherein a secret algorithm defines a mapping between the serial number and a pattern of the pseudorandom copy-resistant printed

Cont B3

marking. The authentication system may further comprise means for executing the secret algorithm and maintaining a security of the secret algorithm, and means for comparing an observed characteristic of a document to be authenticated to an output of the executing means.

On page 56, line 8, to page 57, line 4, amend the paragraph to read as follows:

It is another object of the invention to provide an infrastructure for generating authenticatable original documents, using relatively standard office equipment. In this case, preprocessed media are distributed through standard distribution channels for office supplies. This media is serialized and a description of apparently non-deterministic characteristics are recorded. The medium, which in this case is paper, for example 16-32 lb. stock, having a low contrast apparently non-deterministic pattern resulting from manufacturing processes, with the recorded description being either a description of a non-deterministic pattern, or a ~~stenangiographic~~ steganographic code hidden in the non-deterministic pattern of the media. The paper is loaded into a printer, with the serial numbers

recorded and entered into a software application executing on a print server device, for example a print driver or print spooler associated with the printer. In the case of self-authenticating documents, for each document printed, the software application prints on the document an encrypted code describing the apparently non-deterministic features of the medium as well as a digital signature of the document content. Since this may occur at an operating system level, application programs need not be modified. The encrypted code may be generated in a number of ways. First, the document content and medium identifier may be transmitted to a remote server, for processing into a digital signature, hashed (irreversible process) with the description of the apparently non-deterministic features of the medium, and encrypted, using a public key-private key algorithm. Preferably, the data is compressed. In this case, the information may also be stored at the remote server for remote verification. Second, a description of the apparently non-deterministic features of the medium may be downloaded from a remote server or a local storage medium, such as a CD-ROM, and processed locally to generate the self-authentication signature. In order to provide system

security, in this case, the description of the apparently non-deterministic features of the medium are preferably output from a secure encryption processor, for example having a decryption algorithm stored in volatile memory with memory purging in the event of tampering, which receives a document content and medium identifier, and outputs an encrypted hashed digital signature of the document content and description of the apparently non-deterministic features of the medium. This processor may be a server connecting to a computer network, a "dongle" device, or the like.

Cont B4

On page 63, amend lines 19-27 to read as follows:

FIG. 3 shows a schematic diagram of a document preprocessing system, and FIG. 6A the corresponding method. Raw stock 1 is scanned 101 by scanner 10 to determine a non-deterministic pattern of fibers 6 within the authentication region 3. This data is then stored 102, for example in temporary memory 11 under control of a ~~processor~~ host computer 15, or in association with an identifier of the stock 1.

B5

In the case of a self-authenticating document, as shown in Fig. 1, the data is then hashed with a digital signature

of the document content 103, defined by a page description language file 12, encrypted, and printed 104 on the face (or obverse) of the document in the encrypted coding region 4.